# REMARKS

Reconsideration of the rejections set forth in the Office action dated 10/3/2003 is respectfully requested under the provisions of 37 CFR §1.111(b).

Claims 1-24 are pending.

Claims 1-24 stand rejected.

Applicant includes herewith a petition for an extension of time.

### *I. Rejections under 35 USC §102(e)*

Claims 1-5, 9, 11-13, 15-19 and 23 stand rejected as being anticipated by Yamamoto (6,078,663).

Applicant respectfully traverses this rejection because the Examiner has not established a prima facie case of anticipation.

A prima facie case of anticipation is established when the Examiner provides a single reference that teaches or enables each of the claimed elements (arranged as in the claim) expressly or inherently as interpreted by one of ordinary skill in the art.

> For a prior art reference to anticipate a claim, the reference must disclose each and every element of the claim with sufficient clarity to prove its existence in the prior art. *See In re Spada*, 911 F.2d 705, 708, 15 USPQ 2d 1655, 1657 (Fed. Cir. 1990) (A[T]he [prior art] reference must describe the applicant=s claimed invention sufficiently to have placed a person of ordinary skill in the field of the invention in possession of it.@ (citations omitted)). Although this disclosure requirement presupposes the knowledge of one skilled in the art of the claimed invention, that presumed knowledge does not grant a license to read into the prior art reference teachings that are not there. ***Motorola, Inc. v. Interdigital Tech. Corp.***, 43 USPQ 2d 1481, 1490 (Fed. Cir. 1997)

Previously presented claim 1 is directed to a method for pricing a cryptographic service (for example, but without limitation, a service for encrypting data). A user who

desires to off-load a cryptographic operation from the user's computer can select a cryptographic service provider to perform the cryptographic operation for the user (by selecting the appropriate cryptographic service). The cryptographic service provider receives a request for the desired service and generates a contract based on a variable pricing scheme and sends the contract to the user. On acceptance of the contract, the user sends information to the cryptographic service provider. The cryptographic service provider then causes the contracted-for cryptographic service to be applied to the user-supplied information and thus satisfy the contract. Thus, the user can off-load the burden of performing the cryptographic service on the information from the user's computer to the cryptographic service.

This aspect of the invention is captured in previously presented **Claim 1**:

A method for pricing a cryptographic service on a network utilizing one or more cryptoservers, comprising:

(a) receiving a request for the cryptographic service from a user utilizing the network, wherein the request is received by a cryptographic service provider;

(b) generating a contract based on a variable pricing scheme in response to the request; and

(c) sending the contract from the cryptographic service provider to the user utilizing the network;

(d) receiving, by the cryptographic service provider, information from the user; and

(e) applying the cryptographic service to the information using the one or more cryptoservers to satisfy the contract.

The Examiner has cited Yamamoto Column 16, lines 20-41 and figures 4 and 11 as teaching steps (d) and (e).

Yamamoto teaches techniques for distributing encrypted information from an information providing center to a user who has agreed to a fee for the providing of the

information as well as the strength of the encryption used to protect the provided information. The information is stored at the information providing center.

Yamamoto teaches: 1) a database at the information providing center; 2) contracting for information from the database at a specified encryption strength, and 3) providing the data so encrypted.

The invention of claim 1 includes the limitations of elements (d) and (e). That is, that the cryptographic service provider receives information *from the user* and that the contracted-for cyptrographic service be applied to *this information* to satisfy the contract.

Nothing in Yamamoto teaches or enables applying a cryptographic service on information provided by the user. Thus, Yamamoto does not anticipate the invention of Claim 1. **Claims 11 and 15** are not anticipated for substantially the same reasons.

**Claims 2-5 and 9** (directly or indirectly) depend on and further limit claim 1 and are thus also not anticipated.

**Claims 12-13** (directly or indirectly) depend on and further limit claim 11 and are thus also not anticipated.

**Claims 16-19 and 23** (directly or indirectly) depend on and further limit claim 15 and are thus also not anticipated.

For these reasons, applicant respectfully traverses the 102(e) rejection of claims 1-5, 9, 11-13, 15-19 and 23.

### *II. Rejections under 35 USC §103(a)*

Claims 6-8, 14, 20-22, and 24 stand rejected as being unpatentable over Yamamoto in view of Coyle (6,269,157).

Claim 10 stands rejected as being unpatentable over Yamamoto in view of Schneier et al (5,956,404).

Applicant respectfully traverses these rejections as a prima facie case of obviousness has not been established for either rejection.

A prima facie of obviousness is established by one or more references that were available to the inventor and that teach a suggestion to combine or modify the references, the combination or modification of which would appear to be sufficient to have made the claimed invention obvious to one of ordinary skill in the art.

**A. The invention of Claim 1**

The problem addressed by the invention of currently presented claim 1 is that of a cryptographic service provider providing a user-selected cryptographic service to be applied on data provided by the user. The service offered by the service provider thus offloading the user's computer of the overhead of performing the cryptographic service (page 15, line 19 – page 16, line 5).

The claimed invention addresses this problem by using a cryptographic service provider that receives a request for the desired cryptographic service, generates a contract based on a variable pricing scheme for that service and sends the contract to the user. On acceptance of the contract, the user sends information to the cryptographic service provider. The cryptographic service provider then causes the contracted-for cryptographic service to be applied to the user-supplied information and thus satisfy the contract. Thus, the user can off-load the burden of performing the cryptographic processing from the user's computer to the cryptographic service (page 16, line 6 – page 17 line 20; page 20, line 17 – page 21, line 30).

The elements of previously presented claim 1 are:

(a) receiving a request for the cryptographic service from a user utilizing the network, wherein the request is received by a cryptographic service provider;

(b) generating a contract based on a variable pricing scheme in response to the request; and

(c) sending the contract from the cryptographic service provider to the user utilizing the network;

(d) receiving, by the cryptographic service provider, information from the user; and

(e) applying the cryptographic service to the information using the one or more cryptoservers to satisfy the contract.

**B. Prior Art**

**Yamamoto** teaches techniques for distributing encrypted information from an information providing center to a user who has agreed to a fee for the providing of the information as well as the strength of the encryption used to protect the provided information. As such, Yamamoto is a provider of encrypted data. Thus, the user is simply contracting for access to encrypted information stored at the providing center where that information is encrypted at a user-contracted-for strength.

Yamamoto's technology provides encrypted information from an information provider. Yamamoto discloses a file server that is enhanced to provide encryption to the information in the served files and where a user can select a trade-off between the strength of the encryption, the amount of time it takes to provide the encrypted data, and the user's cost. Yamamoto does not provide a user with any mechanism to apply a cryptographic service to user-supplied information.

Yamamoto does not teach, nor does it teach a suggestion of the limitation within steps (d) or (e) of the present claim 1. In particular, Yamamoto does not teach nor teach a suggestion of applying a selected cryptographic service to information received from the user.

**Coyle.** The Coyle reference teaches a computerized bidding system for selecting telecommunication carriers. The bid information can be encrypted (Coyle, Column 13, lines 30-45). Coyle addresses the problem of electronically determining the best carrier for telecommunications balancing cost, available capacity, and quality of service.

Coyle does not teach, nor does it teach a suggestion of the limitation within steps (d) or (e) of the present claim 1. In particular, Coyle does not teach nor teach a

suggestion of applying a selected cryptographic service to information received from the user.

**Schneier**. The Schneier reference teaches method of creating a digital signature and discloses that public-key encryption, digital signatures, and one-way has functions that are well known in the art.

Coyle does not teach, nor does it teach a suggestion of the limitation within steps (d) or (e) of the present claim 1. In particular, Coyle does not teach applying a selected cryptographic service to information received from the user.

Neither Yamamoto, Coyle, nor Schneier, separately or combined, teach or teach a suggestion of a cryptographic service provider who receives a request for a cryptographic service, that generates a contract for the service based on a variable pricing scheme, that sends the generated contract to a user, that receives information from the user and that applies the selected cryptographic service to the received information to satisfy the contract.

Thus, previously presented claim 1 is patentable. Claims 11 and 15 are patentable for similar reasons.

**Claims 6-8, 14, 20-22 and 24** depend on (either directly or through intervening claims) previously presented independent claims 1, 11, or 15. Thus, claims 6-8, 14, 20-22 and 24 are also patentable.

**Claim 10** depends on presented independent claim 1 through intervening dependent claims. Thus, claim 10 is also patentable.

Since all rejections, objections and requirements contained in the outstanding official action have been fully answered or traversed and shown to be inapplicable to the present claims, it is respectfully submitted that reconsideration is now in order under the provisions of 37 CFR §1.111(b) and such reconsideration is respectfully requested. Upon reconsideration, it is also respectfully submitted that this application is in condition for allowance and such action is therefore respectfully requested.

Should any additional issues remain, or if I can be of any additional assistance, please do not hesitate to contact me at (650) 812-4259.

Respectfully submitted,

Daniel B. Curtis
Attorney for Applicants
Reg. No. 39,159
(650) 812-4259
dbcurtis@parc.com